

What is a Trojan Horse?

McAfee states:

“A Trojan Horse commandeers your hard drive and allows cyber criminals to remotely access to your computer”

Symantec defines a Trojan Horse as:

“¹Trojan horses are impostors—files that claim to be something desirable but, in fact, are malicious. A very important distinction between Trojan horse programs and true viruses is that they do not replicate themselves. Trojan horses contain malicious code that when triggered cause loss, or even theft, of data. For a Trojan horse to spread, you must invite these programs onto your computers; for example, by opening an email attachment or downloading and running a file from the Internet. Trojan.Vundo is a Trojan horse.”

A more common definition of Trojan Horse from ²Webopedia:

“A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer

The term comes from the Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Trojan horses are broken down in classification based on how they breach systems and the damage they cause. The seven main types of Trojan horses are:

- Remote Access Trojans
- Data Sending Trojans
- Destructive Trojans
- Proxy Trojans
- FTP Trojans
- security software disabler Trojans
- denial-of-service attack (DoS) Trojans

Abbreviated as RATs, a Remote Access Trojan is one of seven major types of Trojan horse designed to provide the attacker with complete control of the victim's system. Attackers usually hide these Trojan horses in games, ³screensavers, and other small programs that unsuspecting users then execute on their PCs.”

¹ <http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999041209131106>

² Online encyclopedia for computer technology and terminology <http://www.webopedia.com>

³ There was a screensaver inside one of the directories on Daniel Testerman's computer. If a Trojan horse is found to be attached to this screensaver then that could explain how the images could have been downloaded to this computer by someone else without Testerman's knowledge or consent.



CompTIA[®]

A⁺ Certified Professional

This certifies that:

Jonathan W Black

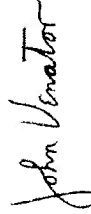
has successfully completed the requirements to be recognized as a:
CompTIA A⁺ Certified Professional

COMP001005810213

Career ID Number

February 28, 2007

Date Certified



John Venator, President/CEO